

## Posudek oponenta bakalářské práce

**Student:** Plaskoň Pavol, Bc.

**Téma:** Rozšíření systému pro shlukovou analýzu binárních souborů (id 20059)

**Oponent:** Ryšavý Ondřej, doc. Ing., Ph.D., UIFS FIT VUT

1. **Náročnost zadání** **obtížnější zadání**  
Jako zadání BP bylo téma obtížnější, neboť vyžadovalo nastudovat principy z oblasti shlukování dat a zároveň pochopení různých současně používaných technologií pro šíření aplikací na platformě Android.
2. **Splnění požadavků zadání** **zadání splněno**  
Zadání bylo splněno realizací rozšíření existujícího systému o možnosti analyzovat nové formáty dat.
3. **Rozsah technické zprávy** **je v obvyklém rozmezí**
4. **Prezentační úroveň předložené práce** **90 b. (A)**  
Práce má vhodnou strukturu. Úvodní kapitola přiměřenou formou představují řešenou problematiku a poskytují motivaci pro uvažované řešení. Kapitola 2 uvádí obecné principy shlukování a uvažované algoritmy. V kapitole 3 je pak představeno prostředí pro shlukovou analýzu vzorků dat společnosti AVG. Kapitola 4 se věnuje představení formátů zdrojových dat. V kapitole 5 je proveden návrh, který je diskutován v následující kapitole popisující implementaci. V kapitole 7 je vyhodnoceno řešení.
5. **Formální úprava technické zprávy** **90 b. (A)**  
Práce má výbornou jazykovou stránku. Text je srozumitelný a obsahuje pouze informace relevantní k řešenému tématu.
6. **Práce s literaturou** **90 b. (A)**  
Autor práce využil relevantní informační zdroje pro téma práce. Vlastní výsledky jsou řádně odlišeny od převzatých informací.
7. **Realizační výstup** **90 b. (A)**  
Realizační výstup byl studentem demonstrován v systému společnosti AVG. Při demonstraci byl plně funkční a poskytoval informace obdobné kvality jako jiné již existující moduly. Integrace modulu do existujícího řešení a jeho používání v běžném režimu dostatečně demonstruje kvalitu realizační části.
8. **Využitelnost výsledků**  
Řešením je praktický nástroj pro shlukování binárních vzorků data reprezentujících podezřelý kód podle jejich význačných charakteristik pro účely následné analýzy. Tento modul se využívá v systému společnosti AVG.
9. **Otázky k obhajobě**
  - Vysvětlíte prosím jak jste postupoval při výběru vhodných vlastností/charakteristik pro shlukovou analýzu. Proč jste vybral zrovna uvedené vlastnosti?
10. **Souhrnné hodnocení** **90 b. výborně (A)**  
Práce se zabývá náročným tématem klasifikace vzorků malware pro jejich následnou analýzu. Autor mě přesvědčil kvalitním zpracováním textové části práce a realizací funkčního netriviálního modulu do existujícího systému.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 30. května 2017

.....  
podpis